

GAO

Testimony

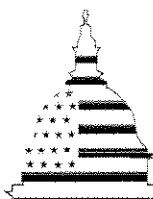
Before the Subcommittee on National
Security, Emerging Threats, and
International Relations, House Committee
on Government Reform

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, April 4, 2006

NUCLEAR POWER

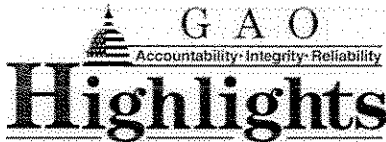
Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve Its Process for Revising the Design Basis Threat

Statement of Jim Wells, Director
Natural Resources and Environment



G A O

Accountability * Integrity * Reliability



Highlights of GAO-06-555T, a testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The nation's commercial nuclear power plants are potential targets for terrorists seeking to cause the release of radioactive material. The Nuclear Regulatory Commission (NRC), an independent agency headed by five commissioners, regulates and oversees security at the plants. In April 2003, in response to the terrorist attacks of September 11, 2001, NRC revised the design basis threat (DBT), which describes the threat that plants must be prepared to defend against in terms of the number of attackers and their training, weapons, and tactics. NRC also restructured its program for testing security at the plants through force-on-force inspections (mock terrorist attacks). This testimony addresses the following: (1) the process NRC used to develop the April 2003 DBT for nuclear power plants, (2) the actions nuclear power plants have taken to enhance security in response to the revised DBT, and (3) NRC's efforts to strengthen the conduct of its force-on-force inspections. This testimony is based on GAO's report on security at nuclear power plants, issued on March 14, 2006 (GAO-06-388).

What GAO Recommends

In its March 2006 report, GAO recommended that NRC improve its process for making changes to the DBT and evaluate and implement measures to further strengthen its force-on-force inspection program.

www.gao.gov/cgi-bin/getrpt?GAO-06-555T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jim Wells at (202) 512-3841 or wellsj@gao.gov.

NUCLEAR POWER

Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve Its Process for Revising the Design Basis Threat

What GAO Found

NRC revised the DBT for nuclear power plants using a process that was generally logical and well-defined. Specifically, trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The resulting DBT requires plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb. Key elements of the revised DBT, such as the number of attackers, generally correspond to the NRC threat assessment staff's original recommendations, but other important elements do not. For example, the NRC staff made changes to some recommendations after obtaining feedback from stakeholders, including the nuclear industry, which objected to certain proposed changes, such as the inclusion of certain weapons. NRC officials said the changes resulted from further analysis of intelligence information. Nevertheless, GAO found that the process used to obtain stakeholder feedback created the appearance that changes were made based on what the industry considered reasonable and feasible to defend against rather than on what an assessment of the terrorist threat called for.

Nuclear power plants made substantial security improvements in response to the September 11, 2001, attacks and the revised DBT, including security barriers and detection equipment, new protective strategies, and additional security officers. It is too early, however, to conclude that all sites are capable of defending against the DBT because, as of March 30, 2006, NRC had conducted force-on-force inspections at 27, or less than half, of the 65 nuclear power plant sites.

NRC has improved its force-on-force inspections—for example, by conducting inspections more frequently at each site. Nevertheless, in observing three inspections and discussing the program with NRC, GAO noted potential issues in the inspections that warrant NRC's continued attention. For example, a lapse in the protection of information about the planned scenario for a mock attack GAO observed may have given the plant's security officers knowledge that allowed them to perform better than they otherwise would have. A classified version of GAO's report provides additional details about the DBT and security at nuclear power plants.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our recent work on security of the nation's 103 operating commercial nuclear power plants, located at 65 sites in 31 states. My testimony today is based on our report being released today, entitled *Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved* (GAO-06-388).¹

As you know, nuclear power plants were among the targets considered in the original plan for the September 11, 2001, terrorist attacks.

Furthermore, according to the Nuclear Regulatory Commission (NRC), which regulates and oversees the safe operation and security of nuclear power plants, there continues to be a general credible threat of a terrorist attack on the nation's commercial nuclear power plants, in particular by al Qaeda and like-minded Islamic terrorist groups. Such an attack could cause a release of radioactive material and endanger public health and safety through exposure to an elevated level of radiation.

To defend against a potential terrorist attack, NRC issues and enforces security-related regulations and orders, and nuclear power plant licensees implement security measures to meet NRC requirements. In particular, NRC formulates a design basis threat (DBT)—the threat that plants must defend against—and tests plants' ability to defend against the DBT. The DBT characterizes the elements of a potential attack, including the number of attackers, their training, and the weapons and tactics they are capable of employing. NRC periodically reviews the potential terrorist threat to determine whether to make changes to the DBT. Most recently, NRC revised the DBT in April 2003 in response to the September 11 terrorist attacks. After revising the DBT, NRC required nuclear power plant sites to submit new security plans by April 29, 2004, for its review and approval and to implement the security described in their new plans by October 29, 2004. In November 2004, NRC began using its force-on-force inspection program to test sites' ability to defend against the revised

¹We also prepared a classified version of our report, which includes additional details about the DBT and security at nuclear power plants that NRC does not release to the public. For more information on NRC's oversight of security at nuclear power plants, see GAO, *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*, GAO-04-1064T (Washington, D.C.: Sept. 14, 2004); and *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: Sept. 4, 2003).

DBT. This program employs mock terrorist attacks as the principal means to test the sites' security.

The DBT does not represent the maximum size and capability of a terrorist attack that is possible but, rather, NRC's assessment of the threat that the nuclear power plants must at all times be prepared to defend against "to ensure adequate protection of public health and safety." Furthermore, NRC regulations do not require nuclear power plants to protect against attacks by an "enemy of the United States," whether a foreign government or other person.² NRC originally included this provision in its regulations in 1967 (prior to issuing the first DBT for nuclear power plants). According to NRC officials, the provision was intended to address the possibility that Cuba might launch an attack on a nuclear power plant in Florida. In revising the DBT in April 2003, NRC did not use this provision to exempt plants from defending against terrorist groups such as al Qaeda but, rather, stated that a private security force (such as at a nuclear power plant) cannot reasonably be expected to defend against all threats—for example, airborne attacks. Importantly, NRC works with other federal agencies to coordinate an integrated response to a terrorist threat or attack on a nuclear power plant.

Our March 2006 report examined (1) the process NRC used to develop the April 2003 DBT for nuclear power plants, (2) the actions nuclear power plants have taken to enhance security in response to the revised DBT, and (3) NRC's efforts to strengthen the conduct of its force-on-force inspections. For the report, we reviewed documents detailing the process NRC used to revise the DBT and interviewed the NRC commissioners and staff. We also visited four nuclear power plant sites (one in each of the four NRC regions) to observe the security enhancements that sites made to address the revised DBT, and we reviewed a sample of NRC's baseline and force-on-force inspection reports. GAO staff with security expertise accompanied us on our visits in order to assist in our review of the sites' security strategies. Finally, we observed a total of three force-on-force inspections at two other sites. We performed our work from November 2004 through January 2006 in accordance with generally accepted government auditing standards.

² 10 C.F.R. § 50.13.

Summary

NRC revised the DBT for nuclear power plants using a process that was generally logical and well-defined. Specifically, trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. To enhance the predictability and consistency of its assessments and its recommendations to the NRC commissioners for changes to the DBT, the NRC threat assessment staff developed and used a comprehensive screening tool to analyze intelligence information and to evaluate particular terrorist capabilities, or “adversary characteristics,” for inclusion in the DBT. The resulting DBT requires plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb. The revised DBT generally, but not always, corresponded to the original recommendations of the threat assessment staff. For example, the maximum number of attackers in the revised DBT is based, in part, on the staff’s analysis of the size of terrorist cells worldwide. However, for other important elements of the DBT, such as the weapons that attackers could use against a plant, the final version of the revised DBT does not correspond to the staff’s original recommendations. We identified the following two principal reasons for these differences:

- First, the threat assessment staff made changes to its initial recommendations after obtaining feedback from stakeholders, including the nuclear industry, on a draft of the DBT. A number of the changes reflected industry objections to the draft. For example, following meetings with industry, the staff decided not to recommend including certain weapons in the list of adversary characteristics that nuclear power plants should be prepared to defend against. In its comments, the industry had pressed for NRC to remove such adversary characteristics from the draft DBT. The industry considered them to be prohibitively expensive to defend against or to be representative of an enemy of the United States, which is the responsibility of the government, rather than the industry, to defend against. NRC officials told us the changes resulted from further analysis of the intelligence data and the reasonableness of required defensive measures rather than the industry objections. Nevertheless, in our view, this situation created the appearance that changes were made based on what industry considered reasonable and feasible to defend against, rather than an assessment of the terrorist threat.
- Second, in deciding on the revised DBT, the commissioners largely supported the staff’s recommendations but also made some significant changes. These changes reflected their policy judgments on what is reasonable for a private security force to defend against. However, the commissioners did not identify explicit criteria for what is and what is not

reasonable for a private security force to defend against, such as the cost of defending against particular adversary characteristics. For example, the commissioners decided against including two weapons that the threat assessment staff had concluded could plausibly be used against a U.S. nuclear power plant. Furthermore, instead of providing a reason for its decision to remove these weapons, the commission's voting record showed that individual commissioners used differing criteria and emphasized different factors, such as cost or practicality of defensive measures. We believe the absence of reviewable criteria reduced the transparency of the decision-making process. The absence of criteria also potentially reduced the rigor of the decision-making process.

Licensees of nuclear power plants have made substantial changes to their security in response to the September 11, 2001, attacks and the 2003 revisions to the DBT. At the sites we visited, these actions included, for example, adding security barriers and detection equipment, implementing new protective strategies, enhancing access control, and hiring additional security officers. In some cases, the sites went beyond what NRC required. For example, one site added electronic intrusion detection equipment to its outer perimeter, which was not required. According to NRC, other sites implemented security enhancements similar to what we saw at the sites we visited. Despite these considerable efforts, it is too early to conclude that all sites are capable of defending against the DBT because, as of March 30, 2006, NRC had conducted force-on-force inspections at 27, or less than half, of the 65 sites. According to NRC, sites have generally performed well during force-on-force inspections, and the results of baseline inspections show that sites have generally complied with their security plans. However, a number of sites have experienced problems and have not always met security requirements. Most notably, we observed a force-on-force inspection at a site in which the licensee's performance at the time was at best questionable in its ability to defend against the DBT.

NRC has made a number of improvements to its force-on-force inspection program. For example, NRC is implementing a schedule to conduct the inspections more frequently at each site—every 3 years rather than every 8 years—and has instituted measures to make the inspections more realistic, such as using laser equipment to better simulate the weapons that attackers and security officers would likely employ during an actual attack on a nuclear power plant. These improvements are important because, as we noted from our observation of three force-on-force inspections and our review of NRC reports on others, the inspections have the ability to detect weaknesses in sites' protective strategies, which can then be corrected.

Nevertheless, in observing three inspections and discussing the program with NRC officials, we noted issues in the force-on-force program that warrant continued NRC attention. For example, the level of security expertise and training among controllers, who observe exercise participants to ensure the safety and effectiveness of the exercises, was inconsistent.

Our report included two recommendations to address the shortcomings in the process NRC used to revise the DBT. First, we recommended that NRC assign responsibility for obtaining feedback from the nuclear industry and other stakeholders on proposed changes to the DBT to an office within NRC other than the threat assessment section, thereby insulating the staff and mitigating the appearance of undue industry influence on the threat assessment itself. Second, we recommended that NRC develop explicit criteria to guide the commissioners in their deliberations to approve changes to the DBT. These criteria should include setting out the specific factors and how they will be weighed in deciding what is reasonable for a private guard force to defend against. In addition, we recommended that NRC continue to evaluate and implement measures to further strengthen the force-on-force inspection program. In commenting on a draft of our report, NRC commended our efforts to ensure that the report was accurate and constructive. NRC also provided additional clarifying comments pertaining to the process it used to revise the DBT for nuclear power plants. For example, NRC requested that we revise the report to explain that it made a deliberate decision to develop the revised DBT while simultaneously seeking input from stakeholders in order to expedite its response to the September 11, 2001 terrorist attacks. We revised the report accordingly.

Background

NRC is an independent agency established by the Energy Reorganization Act of 1974 to regulate the civilian use of nuclear materials. It is headed by a five-member commission, with one commission member designated by the President to serve as chairman and official spokesperson. The commission as a whole formulates policies and regulations governing nuclear reactor and materials safety and security, issues orders to licensees, and adjudicates legal matters brought before it. Security for commercial nuclear power plants is addressed by NRC's Office of Nuclear Security and Incident Response. This office develops policy on security at nuclear facilities and is the agency's security interface with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, the Department of Energy (DOE), and other agencies. Within this office, the Threat Assessment Section assesses

security threats involving NRC-licensed activities and develops recommendations regarding the DBT for the commission's consideration.

The DBT for radiological sabotage applied to nuclear power plants identifies the terrorist capabilities (or "adversary characteristics") that sites are required to defend against. The adversary characteristics generally describe the components of a ground assault and include the number of attackers; the size of a vehicle bomb; and the weapons, equipment, and tactics that could be used in an attack. Other threats in the DBT include a waterborne assault and the threat of an insider. The DBT does not include the threat of an airborne attack.

Force-on-force inspections are NRC's performance-based means for testing the effectiveness of nuclear power plant security programs. These inspections are intended to demonstrate how well a nuclear power plant might defend against a real-life threat. In a force-on-force inspection, a professional team of adversaries attempts to reach specific "target sets" within a nuclear power plant that would allow them to commit radiological sabotage. These target sets represent the minimum pieces of equipment or infrastructure an attacker would need to destroy or disable in order to commit radiological sabotage that results in an elevated release of radioactive material to the environment. NRC also conducts baseline inspections at nuclear power plants. During these inspections, security inspectors examine areas such as officer training, fitness for duty, positioning and operational readiness of multiple physical and technical security components, and the controls the licensee has in place to ensure that unauthorized personnel do not gain access to the protected area. NRC's policy is to conduct a baseline inspection at each site every year, with the complete range of baseline inspection activities conducted over a 3-year cycle. For both force-on-force and baseline inspections, licensees are responsible for immediately correcting or compensating for any deficiency in which NRC concludes that security is not in accordance with the approved security plans or other security orders.

NRC's Process for Revising the DBT Was Generally Logical and Well Defined, but Some Changes Were Not Clearly Linked to an Analysis of the Terrorist Threat

The process by which NRC revised the DBT for nuclear power plants was generally logical and well defined in that trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The NRC commissioners evaluated the recommendations and considered whether the proposed changes constituted characteristics representative of an enemy of the United States, or were otherwise not reasonable for a private security force to defend against. However, while the final version of the revised DBT generally corresponded to the original recommendations of the threat assessment staff, some elements did not, which raised questions about the extent to which the revised DBT represents the terrorist threat.

NRC's Process for Revising Its DBT Was Generally Logical and Well Defined

NRC made its 2003 revisions to the DBT for nuclear power plants using a process that the agency has had in place since issuing the first DBT in the late 1970s. In this process, NRC staff trained in threat assessment use reports and secure databases provided by the intelligence community to monitor information on terrorist activities worldwide. (NRC does not directly gather intelligence information but rather receives intelligence from other agencies that it uses to formulate the DBT for nuclear power plants.) The staff analyze this information both to identify specific references to nuclear power plants and to determine what capabilities terrorists have acquired and how they might use those capabilities to attack nuclear power plants in the United States. The staff normally summarize applicable intelligence information and any recommendations for changes to the DBT in semiannual reports to the NRC commissioners on the threat environment.

In 1999, the NRC staff began developing a set of criteria—the adversary characteristics screening process—to decide whether to recommend particular adversary characteristics for inclusion in the DBT and to enhance the predictability and consistency of their recommendations. The staff use initial screening criteria to exclude from further consideration certain adversary characteristics, such as those that would more likely be used by a foreign military than by a terrorist group. For adversary characteristics that pass the initial round of screening, the threat assessment staff apply additional screening factors, such as the type of terrorist group that demonstrated the characteristic. For example, the staff consider whether an adversary characteristic has been demonstrated by transnational or terrorist groups operating in the United States, or by terrorist groups that operate only in foreign countries. Finally, on the basis of their analysis and interaction with intelligence and other agencies, the staff decide whether to recommend that the commission include the

adversary characteristics in the DBT for nuclear power plants. NRC's Office of Nuclear Security and Incident Response, which includes the Threat Assessment Section, reviews and endorses the threat assessment staff's analysis and recommendations.

Terrorist attacks have generally occurred outside the United States, and intelligence information specific to nuclear power plants is very limited. As a result, one of the NRC threat assessment staff's major challenges has been to decide how to apply this limited information to nuclear power plants in the United States. For example, one of the key elements in the revised DBT, the number of attackers, is based on NRC's analysis of the group size of previous terrorist attacks worldwide. According to NRC threat assessment staff, the number of attackers in the revised DBT falls within the range of most known terrorist cells worldwide.³ NRC staff recommendations regarding other adversary characteristics also reflected the staff's interpretation of intelligence information. For example, the staff considered a range of sizes for increasing the vehicle bomb in the revised DBT and ultimately recommended a size that was based on an analysis of previous terrorist attacks using vehicle bombs. Intelligence and law enforcement officials we spoke with did not have information contradicting NRC's interpretation regarding the number of attackers or other parts of the NRC DBT but did point to the uncertainty regarding the size of potential attacks and the relative lack of intelligence on the terrorist threat to nuclear power plants.

In addition to analyzing intelligence information, NRC monitored and exchanged information with DOE, which also has a DBT for comparable facilities that process or store radiological materials and are, therefore, potential targets for radiological sabotage.⁴ However, while certain aspects of the two agencies' DBTs for radiological sabotage are similar, NRC generally established less rigorous requirements than DOE—for example, with regard to the types of equipment that could be used in an attack. The DOE DBT includes a number of weapons not included in the NRC DBT. Inclusion of such weapons in the NRC DBT for nuclear power plants

³In this report, "terrorist cell" refers only to terrorists who participate in an attack, not those who support but do not participate in an attack.

⁴For further information on the DOE DBT, see GAO, *Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat*, GAO-05-611 (Washington, D.C.: July 15, 2005); and *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: Apr. 27, 2004).

would have required plants to take substantial additional security measures. Furthermore, DOE included other capabilities in its DBT that are not included in the NRC DBT. Despite these differences, both agencies used similar intelligence information to derive key aspects of their DBTs. For example, both DOE and NRC based the number of attackers on intelligence on the size of terrorist cells, and DOE officials told us they used intelligence similar to NRC's to derive the number of attackers. Likewise, DOE and NRC officials provided us with similar analyses of intelligence information on previous terrorist attacks using vehicle bombs. DOE and NRC officials also told us that most vehicle bombs used in terrorist attacks are smaller than the size of the vehicle bomb in NRC's revised DBT.

Changes to the Threat Assessment Staff's Initial Recommendations Were Not Clearly Linked to an Analysis of the Terrorist Threat

While NRC followed a generally logical and well-defined process to revise the DBT for nuclear power plants, two aspects of the process raised a fundamental question—the extent to which the DBT represents the terrorist threat as indicated by intelligence data compared with the extent to which it represents the threat that NRC considers reasonable for the plants to defend against. These two aspects were (1) the process NRC used to obtain stakeholder feedback on a draft of the DBT and (2) changes made by the commissioners to the NRC staff's recommended DBT.

With regard to the first aspect, the process NRC used to obtain feedback from stakeholders, including the nuclear industry, created the appearance of industry influence on the threat assessment regarding the characteristics of an attack. NRC staff sent a draft DBT to stakeholders in January 2003, held a series of meetings with them to obtain their comments, and received written comments. NRC specifically sought and received feedback from the nuclear industry on what is reasonable for a private security force to defend against and the cost of and time frame for implementing security measures to defend against specific adversary characteristics. During this same period, the threat assessment staff continued to analyze intelligence information and modify the draft DBT.

In its written comments on the January 2003 draft DBT, the Nuclear Energy Institute (NEI), which represents the nuclear power industry, objected to a number of the adversary characteristics the NRC staff had included. Subsequently, the NRC staff made changes to the draft DBT,

which they then submitted to the NRC commissioners.⁵ The changes made by the NRC staff—in particular, the size of the vehicle bomb and list of weapons that could be used in an attack—reflected some (but not all) of NEI's objections. For example, NEI wrote that some sites would not be able to protect against the size of the vehicle bomb proposed by NRC because of insufficient land for installation of vehicle barrier systems at a necessary distance. Instead, NEI agreed that it would be reasonable to protect against a smaller vehicle bomb. Similarly, NEI argued against the inclusion of certain weapons because of the cost of protecting against the weapons. NEI wrote that such weapons (as well as the vehicle bomb size initially proposed by the NRC staff) would be indicative of an enemy of the United States, which sites are not required to protect against under NRC regulations. In its final recommendations to the commissioners, the NRC staff reduced the size of the vehicle bomb to the amount NEI had proposed and removed a number of weapons NEI had objected to. On the other hand, NRC did not make changes that reflected all of the industry's objections. For example, NRC staff did not remove one particular weapon NEI had objected to, which, according to NRC's analysis, has been a staple in the terrorist arsenal since the 1970s and has been used extensively worldwide.

With regard to the commissioners' review and approval of the NRC staff's recommendations, the commissioners largely supported the staff's recommendations but also made some significant changes that reflected policy judgments. Specifically, the commissioners considered whether any of the recommended changes to the DBT constituted characteristics representative of an enemy of the United States, which sites are not required to protect against under NRC regulations. In approving the revised DBT, the commission stated that nuclear power plants' civilian security forces cannot reasonably be expected to defend against all threats, and that defense against certain threats (such as an airborne attack) is the primary responsibility of the federal government, in coordination with state and local law enforcement officials. Based on such considerations, the commission voted to remove two weapons the NRC staff had recommended for inclusion in the revised DBT based on its threat assessment. However, the document summarizing the commission's decision to approve the revised DBT did not provide a reason for excluding these weapons. For example, the commission did not indicate

⁵The NRC staff submitted their final draft DBT to the commissioners for their review and approval in April 2003, together with a summary of stakeholder comments.

whether its decision was based on criteria, such as the cost for nuclear power plants to defend against an adversary characteristic or the efforts of local, state, and federal agencies to address particular threats. In our view, the lack of such criteria reduced the transparency of the commission's decisions to make changes to the threat assessment staff's recommendations.

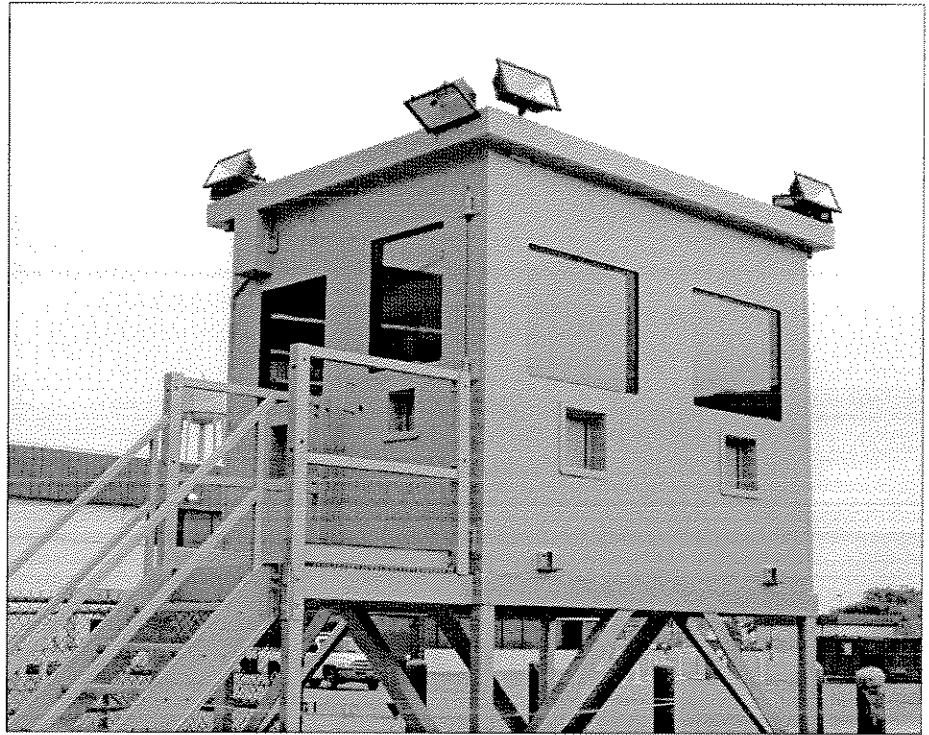
Nuclear Power Plants Made Substantial Changes to Their Security to Address the Revised DBT, but NRC Inspections Have Uncovered Problems

The four nuclear power plant sites we visited made substantial changes in response to the revised DBT, including measures to detect, delay, and respond to the increased number of attackers and to address the increased vehicle bomb size. These security enhancements were in addition to other measures licensees implemented—such as stricter requirements for obtaining physical access to nuclear power plants—in response to a series of security orders NRC issued after September 11, 2001. According to NEI, as of June 2004, the cost of security enhancements made since September 11, 2001, for all sites amounts to over \$1.2 billion.

To enhance their detection capabilities, the four sites we visited installed additional cameras throughout different areas of the sites and instituted random patrols in the owner-controlled areas.⁶ Furthermore, the sites we visited installed a variety of devices designed to delay attackers and allow security officers more time to respond to their posts and fire upon attackers. The sites generally installed these delay devices throughout the protected areas as well as inside the reactor and other buildings. Sites also enhanced their ability to respond to an attack by constructing bullet-resistant structures at various locations in the protected area or within buildings, increasing the minimum number of security officers defending the sites at all times, and expanding the amount of training provided to them. (See fig. 1 for an example of a bullet-resistant structure.) According to NRC, other sites took comparable actions to defend against the revised DBT.

⁶The owner-controlled area refers to the land and buildings within the site boundary that the owner can limit or allow access to for any reason. The protected area is within the owner-controlled area and requires a higher level of access control. The vital area contains the sites' vital equipment, the destruction of which could directly or indirectly endanger public health and safety through exposure to radiation.

Figure 1: Example of a Bullet-Resistant Structure



Source: Nuclear Regulatory Commission.

In addition to adding measures designed to detect, delay, and respond to an attack, the licensees at the four sites we visited installed new vehicle barrier systems to defend against the larger vehicle bomb in the revised DBT. In particular, the licensees designed comprehensive systems that included sturdy barriers to (1) prevent a potential vehicle bomb from approaching the sites and (2) channel vehicles to entrances where security officers could search them for explosives and other prohibited items. The vehicle barrier systems either completely encircled the plants (except for entrances manned by armed security officers) or formed a continuous barrier in combination with natural or manmade terrain features, such as bodies of water or trenches, that would prevent a vehicle from approaching the sites.

In general, the four sites we visited all implemented a “defense-in-depth” strategy, with multiple layers of security systems that attackers would have to defeat before reaching vital areas or equipment and destroying or disabling systems sufficient to cause an elevated release of radiation off

site. The sites varied in how they implemented these measures, primarily depending on site-specific characteristics such as topography and on the degree to which they planned to interdict attackers within the owner-controlled area and far from the sites' vital area, as opposed to inside the protected area but before they could reach the vital equipment. For example, one site with a predominantly external strategy installed an intrusion detection system in the owner-controlled area so that security officers would be able to identify intruders as early as possible. The site was able to install such a system because of the large amount of open, unobstructed space in the owner-controlled area. In contrast, security managers at another site we visited described a protective strategy that combined elements of an external strategy and an internal strategy. For example, the site identified "choke points"—locations attackers would need to pass before reaching their targets—inside the protected area and installed bullet-resistant structures at the choke points where officers would be waiting to interdict the attackers. NRC officials told us that licensees have the freedom to design their protective strategies to accommodate site-specific conditions, so long as the strategies satisfy NRC requirements and prove successful in a force-on-force inspection.

In addition to the security enhancements we observed, security managers at each site described ways in which they had exceeded NRC requirements and changes they plan to make as they continue to improve their protective strategies. For example, security managers at three of the sites we visited told us the number of security officers on duty at any one shift exceeded the minimum number of security officers that NRC requires be dedicated to responding to attacks. Similarly, in at least some areas of the sites, the new vehicle barrier systems were farther from the reactors and other vital equipment than necessary to protect the sites against the size of vehicle bomb in the revised DBT.

Despite the substantial security improvements we observed at the four sites we visited, it is too early to conclude, either from NRC's force-on-force or baseline inspections, that all nuclear power plant sites are capable of defending against the revised DBT for the following two reasons:

- First, as of March 30, 2006, NRC had completed force-on-force inspections at 27 of the 65 sites, and it is not planning to complete force-on-force inspections at all sites until 2007, in accordance with its 3-year schedule. NRC officials told us that plants have generally performed well during force-on-force inspections. However, we observed a force-on-force inspection at one site in which the site's ability to defend against the DBT was at best questionable. The site's security measures appeared

impressive and were similar to those we observed at other sites. Nevertheless, some or all of the attackers were able to enter the protected area in each of the three exercise scenarios. Furthermore, attackers made it to the targets in two of the scenarios, although the outcomes of the two scenarios were called into question by uncertainties regarding whether the attackers had actually been neutralized before reaching the targets. As a result, NRC decided to conduct another force-on-force inspection at the site, which we also observed. The site made substantial additional security improvements—at a cost of \$37 million, according to the licensee—and NRC concluded after the second force-on-force inspection that the site had adequately defended against a DBT-style attack.

- Second, we noted from our review of 18 baseline inspection reports and 9 force-on-force inspection reports that sites have encountered a range of problems in meeting NRC's security requirements. NRC officials told us that all sites have implemented all of the security measures described in their new plans submitted in response to the revised DBT. However, 12 of the 18 baseline inspection reports and 4 of the 9 force-on-force inspection reports we reviewed identified problems or items needing correction. For example, during two different baseline inspections, NRC found (1) an intrusion detection system in which multiple alarms were not functioning properly, making the entire intrusion detection system inoperable, according to the site, and (2) three examples of failure to properly search personnel entering the protected area, which NRC concluded could reduce the overall effectiveness of the protective strategy by allowing the uncontrolled introduction of weapons or explosives into the protected area. According to NRC, the licensees at these two sites, as well as at the other sites where NRC inspection reports noted other problems, took immediate corrective actions.

NRC Has Significantly Improved the Force-on-Force Inspection Program, but Challenges Remain

NRC has made a number of improvements to the force-on-force inspection program, several of which address recommendations we made in our September 2003 report on NRC's oversight of security at commercial nuclear power plants. We had made our recommendations when NRC was restructuring the force-on-force program to provide a more rigorous test of security at the sites in accordance with the DBT, which was also under revision. For example, we recommended that NRC conduct the inspections more frequently at each site, use laser equipment to better simulate attackers' and security officers' weapons, and require the inspections to make use of the full terrorist capabilities stated in the DBT. Actions NRC has taken that satisfy these recommendations include conducting the exercises more frequently at each site (every 3 years rather than every 8 years), and NRC so far is on track to complete the first round

of force-on-force inspections on schedule, by 2007. Furthermore, NRC is using laser equipment to simulate weapons, and the attackers in the force-on-force exercise inspections that we observed used key adversary characteristics of the revised DBT, including the number of attackers, a vehicle bomb, a passive insider, and explosives.

Nevertheless, we identified issues in the force-on-force inspection program that could affect the quality of the inspections and that continue to warrant NRC's attention. For example, the level of security expertise and training among controllers—individuals provided by the licensee who observe each security officer and attacker to ensure the safety and effectiveness of the exercise—varied in the force-on-force inspections we observed. One site used personnel with security backgrounds while another site used plant employees who did not have security-related backgrounds but who volunteered to help. In its force-on-force inspection report for this latter site, NRC concluded that the level of controller training contributed to the uncertain outcome of the force-on-force exercises, which resulted in NRC's conducting a second force-on-force inspection at the site.

Furthermore, we noted that the force-on-force exercises end when a site's security force successfully stops an attack. Consequently, at sites that successfully defeat the mock adversary force early in the exercise scenario, NRC does not have an opportunity to observe the performance of sites' internal security—that is, the strategies sites would use to defeat attackers inside the vital area. When we raised this issue, NRC officials appeared to recognize the benefit of designing the force-on-force inspections to test sites' internal security strategies but said that doing so would require further consideration of how to implement changes to the force-on-force inspections. Based on our observations of three force-on-force inspections, other areas where NRC may be able to make further improvements included the following:

- ensuring the proper use of laser equipment;
- varying the timing of inspection activities, such as the starting times of the mock attacks, in order to minimize the artificiality of the inspections;
- ensuring the protection of information about the planned scenarios for the mock attacks so that security officers do not obtain knowledge that would allow them to perform better than they otherwise would; and

-
- providing complete feedback to licensees on NRC inspectors' observations on the results of the force-on-force exercises.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or the other Members of the Subcommittee may have at this time.

GAO Contact and Staff Acknowledgments

For further information about this testimony, please contact me at (202) 512-3841 (or at wellsj@gao.gov). Raymond H. Smith, Jr. (Assistant Director), Joseph H. Cook, Carol Herrnsstadt Shulman, and Michelle K. Treistman made key contributions to this testimony.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548